
From: "Alex Deas" <ardeas@ibm.net>
To: "Martin Parker" <MartinParker@dialin.net>
Sent: 09 June 2000 23:53
Subject: Handset tried to do a calibration well into a dive

Dear Martin,

My handset said "Dive now? Confirm" when I switched from 0.7 to the 1.30 setpoint 60ft underwater on Thursday. I switched to bail-out immediately and then hit Confirm to see what would happen. It did try a calibration!

I was diving in Scapa Flow on 8th June, planned depth 120ft, using one handset only. The other handset was dead: it has been intermittent for a while - when I switch the handsets on, the right one fails to come on sometimes. I have replaced batteries, cleaned contacts etc, all to no avail. The unit does not stop you diving with one handset down, thankfully. The batteries had been replaced earlier in the week. I did all the other checks (pos and neg pressure, calibrated to 98% O2 at 1000mb).

While swimming to the shot line, I checked PPO2 was within the range 0.5 to 0.6, waited at the top of the shot for it to hit 0.70, then descended fairly slowly - there were three other divers ahead taking their time. On the descent, checked the handset twice - the solenoids stop for longer than normal of course because the PPO2 is rising. I went to do the switch to 1.30, looked at my handset and it said 0.65 to 0.71 on the cells, I pressed the middle button to do the switch but instead of the high set point appearing, I got the Dive Now? display. I immediately switched to bail out, as I did not know what I was breathing with this display. As an experiment, I hit Confirm, and got the Calibrate display. I did not try saying yes. I did a controlled ascent to the surface on OC, then thinking the boat may be a while picking me up, got back onto the RB by switching everything off, back on again, saying Calibrate NO. The unit then gave me the 0.70 setpoint, and I stayed on the RB until the boat picked me up. On deck I checked the unit several times (all still one handset), then after about 10 minutes, did the dive again. This time all was OK.

I can understand how this can happen. I have not seen the circuit diagram for the unit, but when you kindly gave us a factory tour, I was surprised that the handset was a field programmable microcontroller and that was about it - I could not see the markings on the device but it looked like a PIC chip from Arizona microsystems - there are lots of others so I may be wrong on this, but it was certainly of that type.

Life critical systems should not use microcontrollers to operate any function because a single bit soft error from the PROM, the instruction RAM, or power disturbances that affect the address counters, can cause the program to jump to any state from any state, such as Dive Now? or Calibrate? from being underwater.

The structure I would have expected for a life critical system would have the microcontroller driving the display and interfacing with the ADCs, but providing inputs to a separate PLA to control the solenoids and to give state inputs to the microcontroller. The microcontroller is then simply interpreting state instructions so any reset or anomaly will not cause a failure. As well as the PLA giving state bits to the microcontroller, it would take as condition inputs the three buttons, comparator levels from the ADC via the microcontroller and any sensor that says whether the unit is underwater.

The reason for the PLA is that PLAs can be designed to be very sparse, with a maximal hamming distance between the state codes for all valid states. For example, a sparsity of 16:1 would allow 3 bit faults to occur without the system jumping to any valid state. The invalid states should be mapped to do raise a line to the microcontroller, that displays something like Abort Dive whilst still giving the PPO2 levels etc, and the next state from any invalid state should be the normal dive mode and an alarm.

No microcontroller can exhibit the fault ruggedness of a PLA. The cost of implementing a PLA, as a CMOS FPGA to minimise power, is negligible.

The design of life critical electronics is very specialised. I was trained for it at Harwell Laboratory, for obvious purposes. Even though I did an BSc Hons, MSc and PhD in electronics, at no other time were these methods covered. If you are interested in taking it further, I would be happy to run through it in more detail with your electronics design engineer.

By the way, I have so far experienced on the Inspiration:

- Both batteries going down with a minute of each other during a dive. Duracells seem to have a nasty end of life characteristic. I now use Panasonic even though they are 30% more expensive. I have also ordered a Cochran Lifeguard.
- Two cells going down (0.0 PPO2 displayed), causing the injectors to go on constantly - the real PPO2 went up to 1.8 despite a flush, before the gas in the LP line between the reg and injector was exhausted - I had shut off the O2 tank on hearing the injectors come on longer than normal. There should be a check for cells with silly readings in the voting logic, so two cells out by miles do not have this effect.
- The freeflow ice-up problems with the Autoair on descent that you know about.
- A leak in the breathing loop due to a cross thread on the O2 inflator: this escaped the positive pressure test - I did not do the neg pressure test on that dive. Literally a pint and a half of water came out at the end of the dive, and the sorb was very wet. Bubbles came from the inflate ring during the dive, but I did not fancy taking it off and reassembling it underwater.
- During a zero vis free descent without a line or anything else, the dil hose came off - I used up a lot of OC gas before it went back on again. Afterwards I also did a fair bit of practise of these blind descents so descent disasters are handled more comfortably.

- Burst hose underwater. The hose had a very sharp radius as it came out of the bottom port of the dil first stage, and this seemed to have stressed the end of the hose. The end of the hose also rubbed the DIN knurled knob every time the tank was refilled.
- O ring failure on the HP port of the dil regulator. I screwed a Cochran pressure sender unit into it: the O ring was on the surface rather than internal. It blew underwater. I shut down O2 and dil, then switched one on at a time to see which it was. With dil down, I just aborted and came up as normal. There was enough pressure despite the leak to inflate the wing on the surface.

Design features that have impressed me:

- Cells totally open circuit or short circuit are detected and prevent a dive.
- If you do an OC ascent the air in the bags expand to blow the dump valve before they damage anything else.

With best regards,

Alex Deas